AES SYMMETRIC SECURITY RANGE

The IPX-AES Module is an encryptor / decryptor core range that efficiently implements in FPGA the Advanced Encryption Standard as specified in the Federal Information Processing publication FIPS-197 of the National Institute of Standards and Technology.

The IPX-AES module can be customized to ensure its optimization for a wide range of specific applications with a design architecture that can be adapted to support from low up to very high bit-rates. Its flexibility allows combining several functions and operating modes on very small footprints.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>OPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES Data and Key sizes</td>
<td>• 128 bits</td>
</tr>
<tr>
<td></td>
<td>• 256 bits</td>
</tr>
<tr>
<td>Functions</td>
<td>• Decryption</td>
</tr>
<tr>
<td></td>
<td>• Encryption</td>
</tr>
<tr>
<td></td>
<td>• Encryption-Decryption</td>
</tr>
<tr>
<td></td>
<td>• Bypass</td>
</tr>
<tr>
<td>Data-stream handling</td>
<td>• Single stream</td>
</tr>
<tr>
<td></td>
<td>• Multiple streams</td>
</tr>
<tr>
<td>Operation modes</td>
<td>• ECB</td>
</tr>
<tr>
<td></td>
<td>• CBC</td>
</tr>
<tr>
<td></td>
<td>• CTR</td>
</tr>
<tr>
<td></td>
<td>• U+V</td>
</tr>
<tr>
<td></td>
<td>• OFB</td>
</tr>
<tr>
<td>Data and key bus widths</td>
<td>• 32 bits</td>
</tr>
<tr>
<td></td>
<td>• 128 bits</td>
</tr>
<tr>
<td></td>
<td>• 256 bits</td>
</tr>
<tr>
<td>Signal clock with asynchronous reset</td>
<td>• 1</td>
</tr>
<tr>
<td>Simple external interface</td>
<td>• Yes</td>
</tr>
<tr>
<td>Modules</td>
<td>• Looped</td>
</tr>
<tr>
<td></td>
<td>• Unrolled</td>
</tr>
<tr>
<td>Pipelined</td>
<td>• Pipelined</td>
</tr>
<tr>
<td></td>
<td>• Un-Pipelined</td>
</tr>
<tr>
<td>Bit rate</td>
<td>• From 350 Mbit/s up to 20 Gbit/s</td>
</tr>
</tbody>
</table>

FUNCTIONS
Addressing keys of 128 or 256 bits, the IPX-AES cores execute decryption only, encryption only, a combination of encryption and decryption functions plus a bypass mode.

DATA-STREAM HANDLING
The IPX-AES cores can handle the data and secret keys in two different ways.
• The Single Stream option consists of a core capable to encrypt/decrypt data with a single key, before a new update of this key.
• The Multiple Stream option is a feature capable to manage multiple ciphering processes together, each based on a different secret key.

CHAINING MODES
The inter-data-block chaining supports all existing modes that can be used separately or combined into a single design: ECB (Electronic Code-Book), CBC (Cipher Block Chaining), CTR (Counter), CFB (Cipher Feedback), and OFB (Output Feedback).

DATA BUSSES
The incoming, outgoing and key data are handled on either common or separate buses. Data bus width can be sized 32, 128 or 256 bits wide. Bus splitting between data stream, key and initialization value enables high bit-rate operations.

CLOCK
The processes use a single clock and can be reset asynchronously. They may be pipelined, looped or unrolled.

INSTRUCTION SET
The whole process is controlled by a simple set of instructions.
These four versions of the IPX-AES are designed specifically to meet Digital Cinema needs, and demonstrate how powerful and efficient IPX-AES can be.

The modules specified are intended for use in Xilinx FPGAs and comply with the Digital Cinema Initiative Requirement Specification V1.1.

In particular, as illustrated, the IPX-AES-L can be used to decrypt a single asset at up to 250 Mbps (e.g., picture, audio or subtitles).

The IPX-AES-MD can manage multiple assets simultaneously at more than 1 Gbps with automatic context swap between decryption processes. Furthermore, while handling mix of encrypted and in-clear asset data, the core maintains a consistent processing delay between the decryption and bypass modes.

The IPX-AES-M can be used to decrypt respectively 2K and 4K uncompressed data between the Media-Block and the projector.

And, thanks to the compactness of the intoPIX IP-core, it is possible to combine asset decryption, JPEG 2000 decoding, picture watermarking and local link encryption in a single and affordable FPGA.

**Table: IPX-AES Specifications**

<table>
<thead>
<tr>
<th>IPX-AES</th>
<th>DC-250Mbps-ASSET DECRYPTOR</th>
<th>DC-1Gbps-MULTI-ASSETS DECRYPTOR</th>
<th>DC-2K LINK-ENCRIPTOR</th>
<th>DC-4K LINK-ENCRIPTOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES Data and Key size</td>
<td>128 bits</td>
<td>128 bits</td>
<td>128 bits</td>
<td>128 bits</td>
</tr>
<tr>
<td>Function</td>
<td>Decryption only</td>
<td>Decryption &amp; Bypass</td>
<td>Encryption only</td>
<td>Encryption only</td>
</tr>
<tr>
<td>Data-stream handling</td>
<td>Single stream</td>
<td>Multiple stream</td>
<td>Single stream</td>
<td>Single stream</td>
</tr>
<tr>
<td>Operation mode</td>
<td>CBC</td>
<td>CBC</td>
<td>CTR</td>
<td>CTR</td>
</tr>
<tr>
<td>Data and key bus width</td>
<td>32 bits</td>
<td>128 bits</td>
<td>128 bits</td>
<td>128 bits</td>
</tr>
<tr>
<td>Synthesized on</td>
<td>Virtex-4 SX35-10</td>
<td>Virtex-4 SX35-10</td>
<td>Virtex-4 SX35-10</td>
<td>Virtex-4 SX35-10</td>
</tr>
<tr>
<td>Slices</td>
<td>300</td>
<td>1300</td>
<td>750</td>
<td>3000</td>
</tr>
<tr>
<td>RAM Block</td>
<td>3</td>
<td>8</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td>Work Frequency</td>
<td>125 MHz</td>
<td>200 MHz</td>
<td>250 MHz</td>
<td>250 MHz</td>
</tr>
<tr>
<td>Encryption/decryption cycle count</td>
<td>44 cycles</td>
<td>11 clock cycles</td>
<td>11 clock cycles</td>
<td>11 clock cycles</td>
</tr>
<tr>
<td>Encryption throughput</td>
<td>363 Mbit/s</td>
<td>2.3 Gbit/s</td>
<td>3 Gbit/s</td>
<td>12 Gbit/s</td>
</tr>
<tr>
<td>Key update cycle count</td>
<td>92 cycles</td>
<td>34 cycles</td>
<td>On the fly</td>
<td>On the fly</td>
</tr>
</tbody>
</table>

Information provided is accurate at the time of publication, however, no responsibility is assumed by intoPIX for its use, nor for any infringements of patents or other rights of third parties that may result from its use. Specifications subject to change without notice. No license is granted by implication or otherwise under any patent or patent rights of intoPIX. Trademarks and registered trademarks are the property of their respective owners.